**Company Name:** MediVault Health

**Industry:** Healthcare Data Management & Analytics

**Description:**MediVault Health specializes in secure data storage, analytics, and digital solutions for healthcare providers. They provide cloud-based platforms that allow hospitals, clinics, and insurance companies to securely store patient data, track patient outcomes, and analyze health trends. MediVault’s primary focus is on ensuring compliance with healthcare regulations (e.g., HIPAA) and providing accessible, yet secure, data storage and analytics solutions tailored for the healthcare industry.

### **Scenario: MediVault Health’s Access Management Processes**

**Overview:**MediVault is concerned about its access management controls and their ability to thwart unauthorized access to sensitive patient data from compromised credentials.They have hired you to assess their existing processes and controls against the NIST 800-53 baseline to identify areas they need to improve upon.

**Access Management:**

1. MediVault has a well-defined role-based access control (RBAC) system in place, which limits the level of access each employee has to patient data. A compromised account would only have access to the data relevant to that employee’s role, which restricts the amount of data exposed if there is a breach.
2. MediVault’s systems are configured to log user activity, making it possible for the security team to identify which records are accessed. The company’s proactive monitoring and regular audits allowed for a quick review of access logs, helping the team identify the source of a breach and which data was compromised.
3. MediVault conducts annual security training for its employees, ensuring they are aware of phishing attacks and other common methods used to compromise credentials. This training helps prevent more widespread misuse of access credentials, as employees recognize the importance of reporting phishing attempts and following secure password practices.
4. Although MFA is implemented, MediVault only requires it for external access (e.g., remote login), not for on-site logins. If compromised credentials belong to an employee working onsite, the lack of MFA for internal access provides an easy entry point.
5. MediVault has a quarterly review process to update access privileges, but the process does not review service accounts, or token-based access, or other privileged access protocols.
6. Some employees have overlapping permissions on shared resources, such as administrative tools and certain datasets, which are not strictly needed for their specific roles. A breached account would potentially have access to a larger-than-necessary set of permissions, increasing the scope of a breach.
7. MediVault doesn’t have an automated access anomaly detection system in place. Such a system could flag unusual access patterns seen in a breach (e.g., multiple data queries outside normal hours) and alert the security team sooner.
8. MediVault lacks a formal process to test access controls regularly. Periodic tests could uncover flaws in their access controls earlier.
9. Although MediVault follows a role-based approach, they do not fully embrace a "least privilege" policy across all systems. Some users have access to resources and data beyond their immediate job requirements.

**Group Activity**:

Manual assessment:

* Based on the above information, determine which controls from the NIST 800-53 r5 framework the company complies with today, and which controls do not. For the non-compliant controls, provide recommendations to bring them into compliance, including process, technology, services, and/or configurations they should implement.

AI assessment:

* Run the AI “agent” to assess the above scenario against the NIST 800-53 r5 framework, to identify the controls that are compliant, not compliant, and recommendations to remediate the control gaps.